International Journal of Electronics Engineering, 2 (2), 2010, pp. 377–380

Designing a Frame Work for Web Application Information Security Architecture

Sumitra Sangwan[1] and Yashwant Singh Sangwan[2]

[1]*CR College Hisar, Haryana, India, E-mail: cksummi@gmail.com.*

[2]*Department of CSE, BRCMCET, Md University Rohtak, Haryana, India, E-mail: yssangwan@gmail.com.*

Abstract: This paper is part of a major research on Designing framework for web Application information security Architecture and methodology for information security. Over the years, the focus of information security evolved from physical security of computer centers to securing information technology systems and networks, to securing business information systems. With the Internet, computers can communicate and share information with other computers outside organization's networks. This meant that the existing security model was inadequate to meet the threats and challenges inherent in this new web technology infrastructure. A new approach to information security framework for web application is needed to meet these security challenges.

1. INTRODUCTION

In this paper we want to discuss about different facets of security in web Application information system as applicable to Service Oriented Architectures (SOA) Security Architecture implementations. First we examine the security requirements and its solution mechanisms. In the context of Web Services, the predominant SOA implementation standard has a crucial role to play. The Web Services architecture is expected to play a prominent role in developing next generation distributed systems. Building dependable systems based on web services.

Security architecture is a major research issue being discussed Computer security has evolved over the years into its various dimensions of today. Through this evolution, the primary security focus of most organizations was in physical protection of their assets.

2. CONCEPTUAL FRAME WORK FOR WEB INFORMATION SECURITY

The web Application information security planning in this paper is based on the conceptual frame work model for managing information security in the enterprise, developed by Nnolim (2007) in another research. In proposing a conceptual frame work as a decomposition of relev ant meta primitives of an information security management meta model. The meta model presents an enterprise focus, and a potential for integration of information security management with other enterprise life cycle processes, such as strategic planning. The decomposition of relevant meta primitives of the information security management meta model, resulting in the conceptual model, is described as follows:

1. Enterprise business strategy and mission are fundamental inputs to the process of determining information security management goals and objectives.
2. The organization influences an information security management program within that organization. An information security management program resides in the organization, and includes an information security management system.
3. An information security management system is part of a security management program,and it fulfils information security management goals and objectives.
4. Information security management system has one or more information security process improvement models, an information security framework, and an information security management process methodology.
5. An information security framework results from strategic planning, requires one or more information security standards, and includes an information security process improvement model. Information security framework is also described by a security framework description, and it identifies one or more security principles.
6. An information security planning model aggregates to strategic planning.
7. An information security process improvement model is part of an information security management system, and has an information security management processmet methodology.security planning model and information security framework in the conceptual model.

3. WEB SERVICE ORIENTED SECURITY ARCHITECTURE

Web Service-Oriented security Architecture (WSOSA) is “a paradigm for organizing and utilizing Distributed capabilities that may beunder the control of different ownership Domains” [3]. i.e. WSOSA is collection of web services, where these services communicate with each other. The communication can involve either simple data passing or it could involve two or more services coordinating some activity. A service is a component participating in a service-oriented architecture that provides functionalities or participate in realizing one or more capabilities. For the last few years, a rise has been observed in research activity in WSOSA, with applications in different sectors . Several new technologies have been introduced and even more are being currently researched and aimed to the future. Service oriented mentality with the purpose of lessening the issues of clients and companies, students and teachers, citizens and Government companies alike has the most influential approach from software engineering point of view that belong either to Software Architecture has been emerging as a discipline over the last decade. A System Software Architecture describes its coarse-grained structure and its properties at a high level. As long as the technology supports those structures and properties, the technology can be considered to implement the architecture, for instance Jini is a technology that supports web Service-Oriented Architectures because it supports the properties of web Service-Oriented Architecture.WSOSA is implemented by technologies other than Web Services, but the terms and concepts have gained recently because of Web Services. For instance, the computer industry has used the term service for about two decades to describe various platforms. Some of the characteristics of W SOSA are supported better by certain technologies than by others. For instance, CORBA (Common Object Request Broker Architecture) and Jini are less interoperable than Web Services, but Jini excels in other properties (though this is arguable), such as discovery. Web Services are fostering interest in and provides the technology to implement WSOSA that enable them to realize their vision. Data Services will be integral to designing, building and maintaining WSOSA applications. A typical data service will provide a set of operation that encapsulate different ways to access business objects of a given type, to simplify data access for consumers of the services. Data services thus enrich the WSOSA model by letting application developers more easily and rapidly understand the enterprises sea of services, facilitating service discovery and reuse. In object oriented and component based programming, security designers could relay on common languages, security models, and technologies in a distributed system to secure both the client and servers transaction and end points for example, EJB clients and servers can assume and use a common J2EE security standard for authentication and authorization for both its client and server. Malicious attackers exploit the seams left betweenthe existing security mechanisms deployed based on outmoded assumptions and reality of the threats to the connected systems on the ground. Research has shown various flaws with XML security related to its reliance on XML for encryption and signature as well as replicating a number of problems in the legacy technologies. Since a large number of emerging security solutions, particularly WS-* rely on XML security mechanisms it is worth revisiting this dependency to see if XMPP or other technology can remedy these issues.. service in a manner prescribed by its description using SOAP (Simple Object Access Protocol) messages, typically conveyedusing HTTP with an XML serialization in conjunction with other Web-related standards. Web Services Security (WS Security) is a mechanism for incorporating security information into SOAP messages. Web Services Security Architectures have three layers viz. Web Service Layer, Web Services Framework Layer (NET or J2EE), Web Server Layer. Web 2.0 increases web based access to data processing particularly on the client side that enables web applications which contain enriched functionality. Web 2.0 technologies have wide range of technologies and protocols which enable Web architectures greater access to data and functions. The technologies include AJAX (Asynchronous JavaScript and XML), XML, JSON (JavaScript Object Notation), SOAP (Simple Object Access Protocol) and WSDL (Web Services Description Language), REST Web API's, Microsoft Silver light, RSS, RDF, and Atom. Web 2.0 vulnerabilities include XML, JavaScript, RSS, AJAX, SOAP, JSON, WSDL, in decreasing order of their attack statistics. In this research, we want to implement security tools to Web Services Architecture in terms of layers and above attacks [6]. Initially, building web services by combing protocols like REST and WS-* will be studied. Later This Web Services will be secured by adding policy, custom authentication, creating client Security Tools, NET Cryptography, Securing Data Access, and Protecting Code. Etc. Services must be designed and composed in a secure manner. In particular, we are concerned with safety properties of service behavior. Services can enforce security policies locally and can invoke other services that respect given security contracts. This call-by-contract mechanism offers a significant set of opportunities, each driving secure ways to compose services. We can correctly plan service compositions in several relevant classes of services and security properties. We can propose a graphical modeling framework based on foundational calculus. possible vulnerabilities. Securing Web Services Architecture: An element of Security for Web Services consists of Authentication, Authorization,Integrity, Non-repudiation, Confidentiality, and Privacy.Properties of Secure Software for Web Services are Predictability of operation, Simplicity of software design and code, correctness, and safety. The challenge for secure web services has these dimensions: Secure Messaging, Protection of resources, Negotiation of

contracts, Trust management.Common attacks against Web Services include: Reconnaissance attacks, Dictionary attack, Forceful browsing attack, Directory traversal attacks, WSDL Scanning, Sniffing,Privilege escalation attempts, Format String attacks, Exploiting unprotected administrator interfaces, Attacks on confidentiality, Registry disclosure attacks, attacks on integrity: Parameter tampering, coercive parsing, schema poisoning, spoofing of UDDI/ebXML messages, Principal spoofing, Routing detours, External entity attack, cannonicalization, intelligent tampering and impersonation, Denial of Service attacks, Flooding attacks, Recursive payloads sent to XML parsers, Oversized payloads sent to XML parsers, Buffer overflow exploits, Race conditions, Symlink attacks, Memory leak exploitation, Command injection, Structured Query Language injection, XML injection, Malicious code attacks, URL String attack, Parameter Tampering, Cross-site scripting, Session Hijacking, Malformed content, Logic Bombs Trapdoors Backdoors[6]. Several standards are establishing a framework for integrating security into domain-specific XML-basedapplications. Inline signatures with the information that they sign. Signed documents are important not only during transmission between parties, but also as a means to prove and enforce accountability and liability. To do so, signed documents must be easily archived, so that both the contents of a document as well as its signatures can be easily retrieved at a later time. XML Digital Signatures supports inline signatures and also allows different signatures for different parts of a document. WS-Security is emerging as the defacto standard for a comprehensive framework for Web Services security. Table 1 below.

Table 1

Security approach	*Example*	*Benefits*	*Disadvantages*
Network	1. Router 2. Firewall 3. Packet 4. Filter	• Limits access to machines that are authorized to operate within a particular network boundary. • Blocks traffic based on IP addresses, protocols, and port assignments. • Is transparent to applications.	• Cannot inspect application traffic. • Does not limit eavesdropping. • Provides authentication and authorization of host machines only.
Transport	1. SSL 2. TLS	• Limits access to resources that are authorized to use a service. • Blocks traffic based on public key certificates. • Digitally encrypts the transmission of data. • Offers point to point security.	• Does not provide end-toend security. • Does not make security credentials available to application. • Provides all-ornothing access control only.
Application	1. Custom 2. Application 3. Software 4. Module	• Limits access to resources that are authorized to use a service. • Blocks traffic based on message contents. • Digitally signs messages. • Digitally encrypts messages.	• Requires knowledge of the application protocols. • Must be individually built or customized for each type of application,

3.2 Web 2.0 Services Ajax Security Architecture Case Study

Web 2.0 increases web based access to data processing particularly on the client side (AJAX Asynchronous JavaScriptand XML) that enables web applications which contain enriched functionality [7]. Web 2.0 technologies have wide range of technologies and protocols which enable Web architectures greater access to data and functions. The technologies include AJAX (Asynchronous JavaScript and XML), XML, JSON (JavaScript Object Notation), SOAP (Simple Object Access Protocol) and WSDL (Web Services Description Language), REST Web API's, Microsoft Silverlight, RSS, RDF and Atom. Web 2.0 vulnerabilities include XML, JavaScript, RSS, AJAX, SOAP, JSON, WSDL, in decreasing order of their attack statistics. We had implemented securing AJAX Web Services issues. In order to design a secure web tier for AJAX applications, we first need to study the architecture of the AJAX architecture. The client running in the user's browser makes requests to theserver using Hypertext Transfer Protocol (HTTP). Theserequests are processed by the Web server processes, such as Servlets, dynamic pages, etc. The response time is returned tothe client in the form of the streams of data. The web services or pages are accessed by the external entities, without any additional work on our part.

4. CONCLUSIONS

In this paper, we discussed research issues of integrating security into software architecture of Service Oriented Architectures Web Services Security Architectures, while providing dependable design solutions. Further work involves comparing SOA Web Services Security

architectures of Sun ONE and Microsoft NET. Dependability is the key factor if service-oriented computing is to become a success story even in critical areas such as public safety or air traffic control. In order to achieve the end-to-end vision of security, the individual security technologies embedded in the architecture.

REFERENCES

[1] Gunnar Peterson, "Security Architecture Blueprint", *Arctec Group LLC*, 2007.

[2] Spyros T. Halkidis, Nikolaos Tsantalis, Alexander Chatizigeorgiou and George Stephanides, "Architectural Risk Analysis of Software Systems Based on Security Patterns", *IEEE Transactions on Dependable and Secure Computing*, **5 (3)**, pp. 129–142, July-September 2008.

[3] Sasikanth Avancha, "A Framework for Trustworthy Service Oriented Computing", ICISS 2008, pp. 124–132.

[4] Ozgur Erol et al., "A Framework for Enterprise Resilience using Service Oriented Architecture Approach", *IEEE Sys Con 2009, 3 rd annual IEEE International Conference*, March 23–26, 2009.

[5] Anoop Singhal and Theodore Winograd, "Guide to Secure Web Services". NIST Draft (800-95), September 2006.

[6] Massimo Bartoletti, Pierpaolo Degano, Gian Luigi Ferrari and Roberto Zunino, "Semantics Based Design for Secure Web Services", *IEEE Transactions on Software Engineering*, **34 (1)**, pp. 33–49, January-February 2008.